CLAIMS

WE CLAIM:

1. A safety controller comprising:

a first and second processing unit communicating on a communication bus, each including a processor and memory, the memory of each of the first and second processing units loadable with a common safety program and input/output variables, wherein the safety program is repeatably executable to read input variables representing inputs from external controlled devices and write output variables representing outputs to external controlled devices;

a coordinator program providing each of the first and second processing units with identical input variables at a predetermined point in the repeated execution of the common safety programs;

a synchronization program executable by the first and second processing units to execute the common safety programs and to compare execution of the common safety programs and to enter a safety state when this execution differs.

2. The safety controller of claim 1 wherein the coordination program provides identical input variables at only a single point in the repeated execution of the common safety programs.

3. The safety controller of claim 1 wherein the predetermined point in the repeated execution of the common safety programs is the start of the common safety programs.

4. The safety controller of claim 1 wherein the synchronization program compares execution of the safety program by comparing output variables generated by the first and second processing unit executing the safety program.

5. The safety controller of claim 4 wherein the safety program is executed repeatedly and wherein the comparison of the output variables is performed at the conclusion of each repeated execution immediately prior to outputting of the output variables to the external controlled device.

6. The safety controller of claim 1 wherein the safety program also executes to generate values of internal variables different from the input and output variables

and wherein the synchronization program compares execution of the safety program by comparing values of internal variables generated by the first and second processing unit executing the safety program.

7. The safety controller of claim 6 wherein the safety program is executed repeatedly and wherein the comparison is performed at a period greater than the repetition period.

8. The safety controller of claim 1 wherein the coordination program stops the common safety programs execution at the predetermined point in the repeated execution of the common safety program until the identical input variables have been provided to the common safety programs.

9. The safety controller of claim 1 wherein identical input variables are provided by copying of input variables from the first processing unit to the second processing unit.

10. The safety controller of claim 1 wherein the communication bus is a backplane having releasable electrical connectors allowing connection of the first and second processing unit to and from the backplane.

11. The safety controller of claim 1 wherein the communications bus is a serial communications network having releasable electrical connectors allowing connection of the first and second processing unit to and from the serial communication bus.

12. The safety controller of claim 1 wherein the first processing unit includes a buffer memory receiving input variables asynchronously and wherein the coordination program copies the buffer memory identically to memory in each of the processing units.

13. The safety controller of claim 1 wherein the synchronization program combines the output variables when the execution of the common safety program

does not differ to produce a single set of output variables transmittable to the controlled device.

14. The safety controller of claim 1 wherein the combination creates a message having one output variable concatenated to the value of the output variable complemented.

15. A safety controller comprising:

a first and second processing unit each including a processor and memory, the memory of each of the first and second processing units loadable with a common safety program and input/output variables, wherein the safety program is repeatably executable to read input variables representing inputs from external controlled devices and write output variables representing outputs to external controlled devices;

a synchronization program executable by the first and second processing units to execute the common safety programs and to compare execution of the common safety programs and to enter a safety state when this execution differs;

wherein the synchronization program compares execution of the safety program by comparing outputs generated by the first and second processing unit executing the safety program at the conclusion of each repeated execution immediately prior to outputting of the output values to the external device.

16. A safety controller comprising:

a first and second processing unit communicating on a communication bus, each including a processor and memory, the memory of each of the first and second processing units loadable with a common safety program and input/output variables, wherein the safety program is repeatably executable to read input variables representing inputs from external controlled devices and write intermediate variables not output to external controlled devices and write output variables representing outputs to external controlled devices;

a synchronization program executable by the first and second processing unit to execute the common safety programs and to compare execution of the common safety programs and to enter a safety state when this execution differs;

wherein the synchronization program compares execution by comparing output variables and intermediate variables at different periods.

17. A method of operating a safety controller having a first and second processing unit, each including a processor and memory, the memory of each of the first and second processing units loadable with a common safety program and input/output variables, the safety program being repeatably executable to read input variables representing inputs from external controlled devices and write output variables representing outputs to external controlled devices, the method comprising the steps of:

(a) providing each of the first and second processing units with identical input variables at a predetermined point in the repeated execution of the common safety programs; and

(b) executing by the first and second processing units the common safety programs and comparing execution of the common safety programs to enter a safety state when this execution differs.

18. The method of claim 17 wherein step (a) provides identical input variables at only a single point in the repeated execution of the common safety programs.

19. The method of claim 17 wherein the predetermined point in the repeated execution of the common safety programs is the start of the common safety programs.

20. The method of claim 17 wherein step (b) compares execution of the safety program by comparing output variables generated by the first and second processing unit executing the safety program.

21. The method of claim 20 wherein the safety program is executed repeatedly and wherein step (b) is performed at the conclusion of each repeated execution immediately prior to outputting of the output variables to the external controlled device.

22. The method of claim 17 wherein the safety program also executes to generate values of internal variables different from the input and output variables and wherein step (b) compares execution of the safety program by comparing values of internal variables generated by the first and second processing unit executing the safety program.

23. The method of claim 26 wherein the safety program is executed repeatedly and wherein the comparison is performed at a period greater than the repetition period.

24. The method of claim 17 wherein step (a) stops the common safety program's execution at the predetermined point in the repeated execution of the common safety program until the identical input variables have been provided to the common safety programs.

25. The method of claim 17 wherein identical input variables are provided by copying of input variables from the first processing unit to the second processing unit.

26. The method of claim 17 wherein the first processing unit includes a buffer memory receiving input variables asynchronously and wherein step (a) copies the buffer memory identically to memory in each of the processing units.

27. The method of claim 17 wherein step (b) combines the output variables when the execution of the common safety program does not differ to produce a single set of output variables transmittable to the controlled device.

28. The method of claim 17 wherein the combination creates a message having one output variable concatenated to the value of the output variable complemented.

29. A method of operating a safety controller having a first and second processing unit each including a processor and memory, the memory of each of the first and second processing units loadable with a common safety program and

input/output variables, the safety program being repeatably executable to read input variables representing inputs from external controlled devices and write output variables representing outputs to external controlled devices;

the method comprising the steps of executing the common safety programs to compare execution of the common safety programs and to enter a safety state when this execution differs where the comparison of execution compares outputs generated by the first and second processing unit executing the safety program at the conclusion of each repeated execution immediately prior to outputting of the output values to the external device.

30. A method of operating a safety controller having a first and second processing unit, each including a processor and memory, the memory of each of the first and second processing units loadable with a common safety program and input/output variables, the safety program being repeatably executable to read input variables representing inputs from external controlled devices and write intermediate variables not output to external controlled devices and write output variables representing outputs to external controlled devices,

the method comprising the steps:

of executing the common safety program on the first and second processing units. and comparing execution of the common safety programs to enter a safety state when this execution differs wherein the comparison compares execution by comparing output variables and intermediate variables at different periods.